Configuring FortiOS v5.0 Webfiltering for HTTPS scanning without SSL Deep Scanning

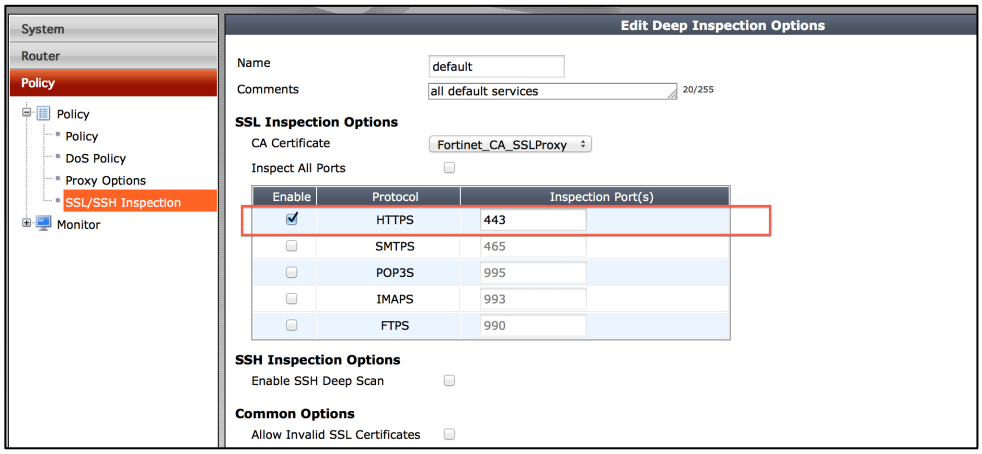
Introduction

The FortiOS FortiGuard Webfiltering and URL Filter can be configured to block or allow HTTPS websites without the need of SSL Deep Inspection. The webfilter daemon has the ability to extract the website's hostname from the SSL Certificate (CN field), which is sent via an unencrypted session (HTTP) before the SSL tunnel is established, and it uses this hostname info to rate the website (not the full URL), thus blocking or allowing access.

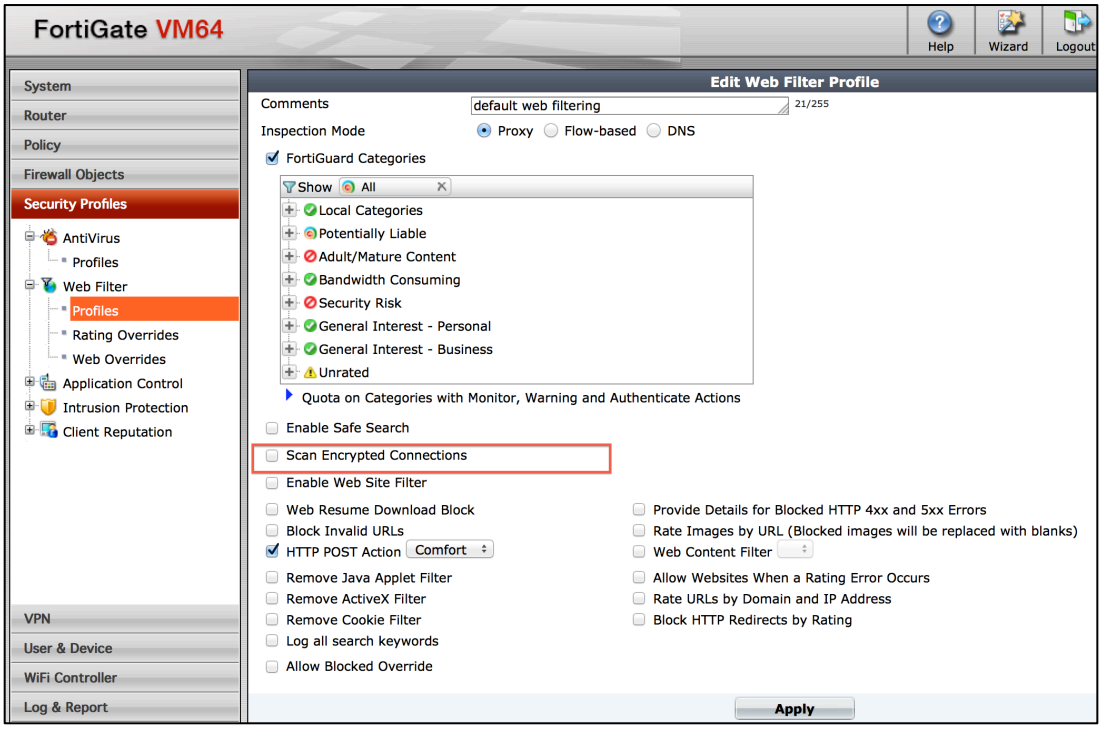
Since SSL Deep Inspection is not necessary, there's no need of installing the Fortigate's self-signed certificate in all workstations or buying a valid certificate for that purpose.

Configuration

1. Create a new SSL/SSH Inspection profile and enable HTTPS over port 443.



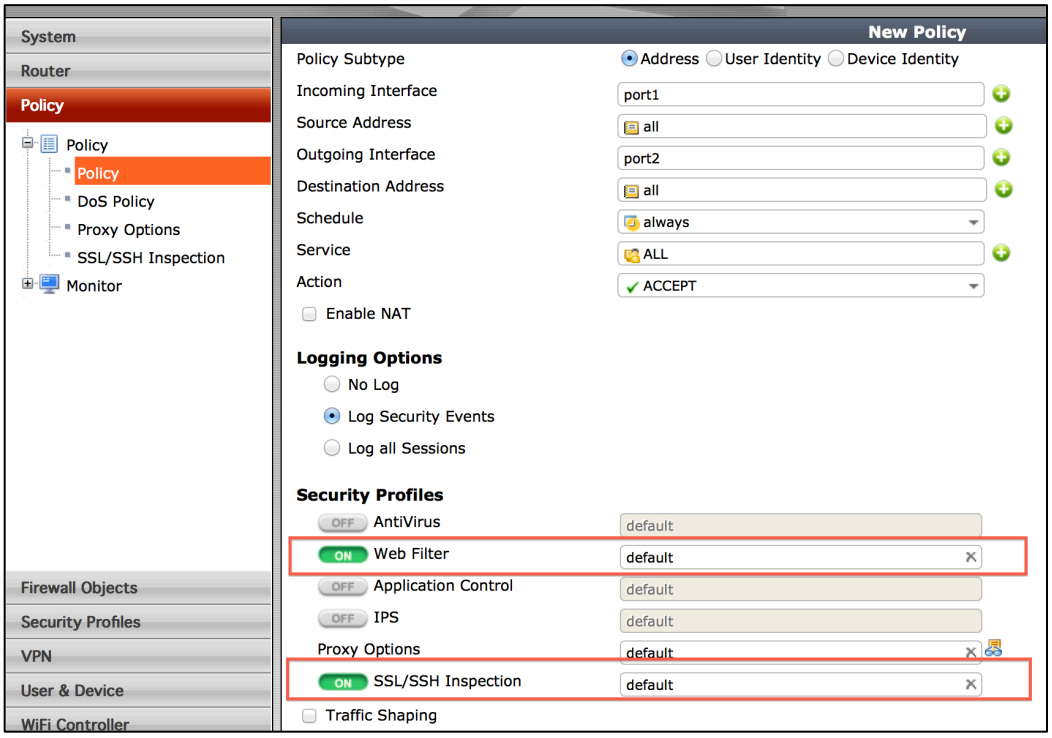
2. Unset the option *Scan Encrypted Connection* under your Webfilter Profile.



This is the same of running the following CLI commands:

```
config webfilter profile
  edit <profile_name>
      set options https-url-scan
  end
end
```

3. Select both SSL/SSH Inspection and Webfilter profiles on your policy that controls HTTPS access.



When configuring the FGT to do this if a webpage is blocked, by default the FGT will send a replacement-message to the user and since it is a HTTPS website, the replacement-message URL will also be via HTTPS. In this case the user will also be asked to accept the FGT's self-signed certificate, but THIS IS ONLY for the replacement-message URL and it does not mean SSL Deep Scanning is enabled.

You can easily test this accessing an allowed HTTPS website and you will see that it won't ask you to accept the FGT's self-signed certificate, while for a blocked website you'll see the certificate warning message on your browser.

There's a CLI command that can disable the replacement-message for HTTPS websites and the browser's time-out message will be showed instead:

```
config webfilter profile
    edit "default"
       set https-replacemsg disable
    end
end
```